Business Impact of Identity Management In Information Technology

Mr. Chris Villemuer& Dr. Syed Adeel Ahmed

Abstract: *This paper explains the importance of data security through identity management. Businesses must do everything practical to protect their data and IT systems from malicious parties. Hackers have many tools and methods at their disposal, such as phishing, to steal identity data and compromise IT systems for malicious purposes. Even failures by an organization's own IT department to protect against malicious use from its own employees have resulted in significant financial losses. These losses could have been prevented had adequate identity management steps been taken. Usage of technologies such as a centralized Identity Management System, Directory Services, or Federated Identity Management protect a user's private information and effectively control access to business systems. Many core IT business systems and cloud service providers can leverage these identity management technologies to provide data security and secure access control.*
Keywords: Identity management, provisioning, access control, credential, user name, password, directory service, federated identity, phishing, identity theft

I. Introduction

Many businesses and organizations must comply with federal rules and regulations to protect data from unauthorized access by malicious parties. Stolen or compromised data can yield severe consequences. These consequences range from financial loss to legal repercussions from local, state, or federal government entities. A robust identity management strategy has become an important concept in controlling access to data in business IT systems (F5, 2016). However, due to lack of unified standards for identity management in many IT systems, effectively controlling identity and access is a challenge for many organizations. Fortunately, there are identity management tools and methods available that can ease burdens for both IT administrators and organizations. This paper discusses the challenges of identity and access management, and methods for overcoming them.

II. Problem

Organizations face technical, social, and operational challenges with identity management. There are key components of identity management that must be addressed to protect an organization and its constituent data. Managing these components of identity management is a challenge for many organizations. Failing to meet these challenges of effective identity management has had severe consequences for government and corporate entities, and especially their customers. There are threats both within and outside of organizations that use various methods of exploiting ineffective identity management practices to compromise IT business systems.

2.1. System Access Control

Businesses often use many application systems to accomplish their goals. Some of these applications are even critical to the success of the business. For example, many business office environments today rely on email as a primary form of communication. Many employees use a centralized email system managed by an IT department. Other critical business application systems used by most companies include Human Resource Management, Payroll, Marketing, etc. Each system has its own means for managing identities and access control that must be managed. Failing to adequately monitor and manage access control increases risk of loss. Inadequate access control invites risk of system abuses from even legitimate employees. For example, the 2011 UBS Rogue Trader Scandal resulted in a staggering $2 billion financial loss for UBS Bank. A single employee with unauthorized access to key trading systems performed securities trades that resulted in financial loss. If IT staff of UBS had adequately enforced access control, the loss could have been prevented (Fogarty, 2011).

2.2. Protecting User Credentials

Most application systems require users to present credentials to access the system. These credentials can be one or a combination of: username/password, smart device, and biometrics. Effectively protecting and managing user credentials in disparate systems is a challenge in Identity Management. Many applications have their own systems for identity management and access control. These systems store user credentials. User name/password is the most common credential form used in many IT systems, and also the most vulnerable. There are various methods available to malicious entities that can be used to steal user credentials.

2.2.1. Phishing

This is arguably the simplest, yet most effective method for maliciously obtaining user credentials. Phishing is the practice of electronically posing as a legitimate system authority to trick users into transferring their credentials, usually for the fictional purpose of system validation or other false validation. From there, malicious entities use these stolen credentials to access systems. Username and password is the most common, and simplest credential to transfer via phishing scams. On November 24, 2014, hackers claimed responsibility for hacking into Sony Pictures Entertainment IT systems. Security firm Cylance identified phishing as the means hackers used to gain credentials to access Sony's systems. The credentials were coded in the "Wiper" malware that was largely responsible for crippling and compromising Sony Picture Entertainment (Bisson, 2015). This incident resulted in significant consequences for Sony Pictures Entertainment. Employee information, financial records, server keys, and other sensitive corporate information was posted publicly by the hackers.

2.2.2. **Identity Theft**

In recent years, identity theft has become a significant threat to both organizations and consumers around the world. Identity theft is the practice of maliciously using a person's identifying information for gain. Examples of applications of stolen identities include unauthorized access to a victim's bank account to steal funds, and unauthorized uses of a victim's credit card to pay for items. These forms of identity theft have both severe impact to both individuals and financial institutions involved. Extracting identity information can be performed in various ways. Hackers can exploit vulnerabilities in IT business system software and use that as means to steal identity information from databases. Even phishing techniques can be used to trick victims into revealing sensitive identifying information about themselves (Douglas, 2016).

III. Method

There are methods and technologies available to effectively manage identities. These methods have been the result of years of collaboration between government, business, and educational institutions. Often, businesses leverage more than one method to effectively manage identity and access across the organization. In most cases this is necessary because there is no single standard or unifying solution to identity management for every IT system. Some business IT systems have specific identity management requirements that only certain solutions can meet. Having a variety of identity management methods available is important to dynamically meet varying system requirements.

3.1. Identity Management Systems

Identity management systems are hardware and/or software systems that manage identity and access control for various other IT systems. Identity management systems contain specific logic for interacting with many types of business application and infrastructure systems. These interactions include processes for common identity management tasks such as: provisioning/deprovisioning user accounts, managing passwords, controlling system access through groups or role-based access methods.

Microsoft Identity Manager (MIM) is a long-standing identity management system used by many organizations. It has gone through numerous product re-names. However, the core functionality has remained the same and been expanded upon over the years (What Is Microsoft Identity Manager (MIM) 2016, 2015). MIM can provision/deprovision user accounts in various popular systems such as Oracle, Office 365, Active Directory. Timely provisioning and deprovisioning of user accounts ensures unauthorized access is not granted to users if their credentials expire. It also provides self-service password management for users. This allows organizations to enforce password policies on users and helps mitigate risks associated with credential theft. Another key feature of MIM is Privileged Access Management (PAM). This ensures users only have necessary access to systems within a specified time window according to their role in an organization. Monitoring and controlling access by a time window helps mitigate risks of unauthorized access from even legitimate user accounts.

3.2. Directory Services

Directory services are lightweight databases that contain structured identity data about a person, place, or entity. LDAP (Lightweight Directory Access Protocol) directories were created around 1993, and have been widely used in IT since then. LDAP is based on the directory X.500 model. A directory entry contains multiple attributes that can be used to identify the entry. This is ideal for identity management as it allows more than one source of information to be used to identify an entity. LDAP entries contain a username and password that is authenticated through an LDAP interface. This allows for centralized storage and access of user credentials in a standardized way. Many business applications can integrate their identity and access mechanisms with entries in LDAP directories. This provides centralized access

control and secure credential storage.

There have been several widely used implementations of LDAP since its inception. Novell eDirectory, OpenLDAP, and Sun LDAP directory server are some of the most popular. However, the most widely used and arguably the most successful is Microsoft Active Directory. In addition to providing centralized LDAP structured data, Active Directory also provides policy enforcement and other built-in mechanisms to provide additional security for identity and access control. Security Groups are a directory entry used specifically for controlling access to AD/LDAP integrated systems. Active Directory also provides a policy enforcement mechanism known a Group Policy. This allows for enforcement of policies and standards on user accounts, as well as the machines these user accounts connect to (Azam, 2012).

3.3. Federated Identity Management

Identity Federation is a relatively new concept in identity management. It has only started to become adopted in the past 5-10 years. Instead of provisioning and managing identity records, federation approaches identity management by leveraging existing records. This allows organizations to use existing identity stores. Federation allows secure sharing of identity information with other organizations, without actually transferring stored user credentials. Organizations establish a secure, federated digital trust relationship. This trust allows organizations to create claims for users. These claims can be used to control access to applications and services hosted by other organizations.

Popular cloud service providers such as Google and Microsoft Office 365 allow customers to create federated trusts to leverage their cloud services. The end result is organizations can take advantage of cloud services while still using their own on premise identity systems to store user credentials and control access. Examples of widely used federated identity management systems include Shibboleth IdP, Gluu, and Microsoft ADFS (Active Directory Federation Services). Shibboleth has been one of the most long-standing federation systems and is still widely used today.

IV. Conclusion

Businesses and organizations of all sizes leverage IT to accomplish their goals. Almost all IT systems require user identities to govern data access. Failing to address effective identity management in IT systems creates significant risk of loss for organizations. Hackers use numerous methods to exploit identity data for malicious purposes. While there is no singular, standard approach to identity management, there are several effective identity management methods available that help mitigate risk. One or a combination of these currently available methods are used by organizations to protect their data, and most importantly their customers. Effective identity management methods must continue to evolve to meet continuing threats of business losses due to inadequate identity and access management practices.

REFERENCES

[1] Azam, W. (2012, December 5). *Active Directory's Introduction and Its Features n Advantages*. Retrieved from W7Cloud: http://www.w7cloud.com/active-directorys-introduction-and-its-advantages/

[2] Bisson, D. (2015, April 22). *Sony Hackers Used Phishing Emails to Breach Company Networks*. Retrieved from Tripwire: http://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

[3] Douglas, R. (2016). *Identity Theft Victim Statistics*. Retrieved from Identity Theft and Scam Prevention Services: http://www.identitytheft.info/victims.aspx

[4] F5. (2016, February 24). *The Challenges and Benefits of Identity and Access Management*. Retrieved from F5 Networks: https://f5.com/resources/white-papers/the-challenges-and-benefits-of-identity-and-access-management-17862

[5] Fogarty, K. (2011, October 7). *UBS admits its security system did spot the trader who lost $2B, but ignored it*. Retrieved from ITWorld: http://www.itworld.com/article/2735514/security/ubs-admits-its-security-system-did-spot-the-trader-who-lost--2b--but-ignored-it.html

[6] *What Is Microsoft Identity Manager (MIM) 2016*. (2015, November 17). Retrieved from NewSignature: http://www.infrascience.com/uncategorized/what-is-microsoft-identity-manager-mim-2016/